Design of Blockchain - Based Algorithm for Cloud Data Security

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna International Institute of Research and Studies

(Deemed to be University)

by

POONAM KUMARI

(19/Ph.D/106)

Under the supervision of

Dr. Meeta Singh

Professor, Computer Science & Engineering

SCHOOL OF ENGINEERING & TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD

SCHOOL OF ENGINEERING & TECHNOLOGY

CERTIFICATE

I hereby declare that the short synopsis "Design of Blockchain-Based Algorithm for Cloud Data Security" being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in Security in Cloud Computing under faculty of Dr. Meeta Singh, Professor, Department of Computer Science & Engineering of Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2019.

It is a bonafide record of original work carried out under the supervision of Dr. Meeta Singh and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is plagiarism free and proof has been submitted.

Poonam Kumari

(19/Ph.D/106) Poonam Kumari

Dr. Meeta Singh

Professor

Department of Computer Science & Engineering

School of Engineering & Technology

Manav Rachna International Institute of Research and Studies (Deemed to be University), Faridabad

Chairperson, DRC

Dean,

School of Engineering & Technology

ABSTRACT

Nowadays, Cloud Computing is the fastest-growing IT technology which is rising day by day because of its flexibility & easy to use features. Cloud Computing provides the ability to reduce the cost of pay-per-use and increases scalability. When a user demands any resource or service like software, hardware, or infrastructure in cloud computing then that will be provided as per the request. The major concern is the data security in cloud computing, as the data will be stored by a third party & easily accessible through the internet. Many security issues can arise due to the invisibility of data as there is no full control over data by the customer. Therefore, there is a need for cloud security which must ensure the protection of the user data on the cloud.

Cloud security contains several policies, procedures, roles, permissions, and use of technology and protects the data on the cloud. Cloud security must be robust so that the user can freely transfer their data to the cloud without any worries. As the data on the cloud is constantly growing day by day which in turn increases the security threats and risks. Because of security threats and risks in the data cloud, security is becoming the latest area of research.

It is essential to use cloud services provided by a cloud provider that ensure the data security. Most writings concentrate on making cloud storage secure enough for confidential data. Today, the Internet of Things (IoT) is utilized to make people's lives simpler in a number of scenarios. Massive volumes of data are generated by the Internet of Things, which must be processed and stored in the cloud. Also, the Blockchain is a distributed ledger; data kept there is safe from prying eyes. It is possible for any internet-connected computing node to join or create a peer network, maximizing the efficiency with which resources are used. Blockchain is a peer-to-peer, decentralized system in which every computer in the network holds its own copy of a blockchain database. As a result, the blockchain's initial state is protected from manipulation. In this configuration, the user's file is encrypted using Interplanetary File System protocol before being transferred to other network peers. In this research, a cryptographic approach will be develop to improve the safety of cloud-based data via the use of blockchain technology in distributed processing content, and will also establish bloom technology as the basis for achieving the highest possible levels of data availability and storage efficiency. Also it will show the efficacy of the approach with respect to the availability and storage of data.

Keywords: Blockchain, Bloom Technology, Cryptography, Internet of Things (IoT), Interplanetary File System

Table of Contents

S. No.	Description	Page No.
1	INTRODUCTION	1-9
	1.1 Characteristics	
	1.2 Deployment Models	
	1.3 Service Delivery Models	
	1.4 Cloud security	
	1.4.1 Challenges of cloud security	
	1.4.2 Types of cloud security	
2	LITERATURE REVIEW	10-15
	2.1 Research Gaps	
3	CLOUD SECURITY USING BLOCKCHAIN	16-18
	3.1 Blockchain Network Types	
	3.2 Problem statement	
4	RESEARCH OBJECTIVES	19
5	RESEARCH METHODOLOGY	20-21
6	EXPECTED OUTCOME	22
	REFERENCES	23-26

1. INTRODUCTION

Cloud Computing continues to experience rapid growth in the field of IT, driven by its inherent flexibility and user-friendly features. Its allure lies in the capacity to lower costs through a pay-per-use model while simultaneously enhancing scalability. In the realm of cloud computing, users can effortlessly access requested resources or services, such as software, hardware, or infrastructure, aligning with their specific needs and demands. It's crucial to recognize that when referring to the "Cloud," are actually addressing cloud computing rather than a physical location. This distinction opens up promising prospects for the dominance of future applications residing predominantly in the cloud. The increasing adoption of cloud computing solutions is driven by the need to meet the escalating demands of business programmers and clients.

The adoption of cloud computing solutions is on the rise to meet the growing demands of numerous business programmers and clients. Examples like Dell EMC and Amazon are favored cloud service providers due to their perceived cost-effectiveness and technical advancement over traditional data centers. However, security remains a significant concern, distinguishing cloud computing from other storage technologies. When company data is transferred to the cloud, the cloud provider assumes responsibility for its security. This introduces overlapping trust boundaries and increased data exposure, potentially providing opportunities for criminal cloud users to target IT systems and steal or corrupt company data. Addressing this security concern, a "Distributed Cloud Model" utilizing blockchain technology can be employed. Many individuals are drawn to blockchain technology for its promise of novel, secure, and affordable options for storing their ever-growing data collections. Blockchain eliminates the need for trusted third parties, initially developed for digital currency like Bitcoin. Moreover, Blockchain data is distributed across multiple locations, creating a peer-to-peer system that is highly resistant to penetration by hackers.

Traditional cloud storage model

In traditional cloud storage architecture, the front-end platform can be a client or mobile device, while the network may consist of the internet or an intranet, and the back-end platform typically comprises servers or storage systems. A prime example of traditional cloud services is Google Drive, where all uploaded files are securely stored in Google data centers (D. Grzonka et al., 2015). When users on mobile devices or computers wish to access their data, they simply send a request to the data center. However, running large data center operations comes with significant

expenses. These data centers require frequent technology updates, along with operational costs for cooling, maintenance, and upgrades. Safety is another crucial consideration (L. Jiang et al., 2022). Despite the implementation of stringent security measures by many cloud providers, there remains a possibility of breaches leading to unauthorized access to sensitive data, as evidenced by incidents like the recent celebrity cloud hack (W. Li et al., 2021). Privacy is also at risk from various sources beyond human error (G. Rathee et al., 2022). Non-encrypted files may be susceptible to scrutiny by major corporations, whose privacy regulations outline various scenarios permitting lawful access and sharing of data (J. Zhu et al., 2018).

1.1 Characteristics

Cloud computing presents a range of crucial attributes that appeal to businesses aiming to expand their operations and improve agility. Features such as flexibility, accessibility, reliability, security, and cost-effectiveness contribute to cloud computing's transformative impact on the technology landscape. Following key characteristics set cloud computing apart from traditional computing models:

i.. Multi-tenancy

Multi-tenancy means sharing the resources. Multiple tenure is very important in cloud computing because many organizations share the data with other organizations on cloud.

ii. Massive scalability

Massive scalability in cloud computing refers to the capability to scale thousands of systems as well as increase bandwidth and storage capacity.

iii. Elasticity

Cloud service providers provide the resources quickly and users scale the resource up and down according to their needs.

iv. Pay to Use

Users can only pay for that resource that they can use and many times users take the resources for rent so that users can only pay for that time resources are being used.

v. Prior provision of resources

The prior provision of resources by the user, that is, it already organizes the system and the additional resource.

1.2 Cloud deployment models

Cloud deployment models are divided into three categories, determined by factors such as accessibility, ownership of the infrastructure, and storage size. The critical considerations in choosing a deployment model revolve around two key parameters: (i) control over the infrastructure and (ii) its geographical location. There are three types of deployment models as follows:

Private cloud

Systems and services are accessible only within the organization. It can also manage third parties**.** In this model, users can store the data in the cloud with a secure private key so that hackers cannot hack the data in the private cloud. Users buy the resources for their own organization and not share them with the other organization. It is only used by people who trust on cloud eg. Microsoft, VMware, Ubuntu.

Public Cloud

In public cloud, cloud service providers share the resources publicly, that is, they share the resource across many organizations. It provides true cloud hosting and services to the various users. Google, Amazon, Microsoft are examples of public cloud. It is provided by a provider at some cost.

Hybrid Cloud

Hybrid cloud is a combination of public and private cloud or public cloud and community cloud and vice versa. It is called a hybrid cloud. In a hybrid cloud, data is safe and uses the secure application. Mostly hybrid clouds rely on the combination of two cloud models.

1.3 Service Delivery Models

"Cloud services" refer to a broad category of Internet-based offerings that may be quickly accessed by anybody, anywhere in the world. These services don't need any special gear or software to run; it may save user’s time and money. Most employees often use cloud services throughout the workday for tasks like checking email and working together on papers.

Management of cloud services is a responsibility that rests solely on the cloud computing vendor or service provider. Rather than having to host applications on their own servers, businesses may simply direct their customers to the servers of the service providers.

There are three different service models for cloud computing, each catering to a different business need. The three main cloud computing concepts are as follows:

Software as a Service (SaaS)

When user uses a service, the software provider is in charge of the program's administration and upkeep of the service's associated web-based solutions. It means that the company can stop stressing about keeping its applications up-to-date, which includes managing software upgrades, network security, architecture, data availability, as well as other similar operational problems. In most cases, the number of users, the cost of utilizing a SaaS depends on a variety of factors, including the customer's data storage needs, transaction volume, and length of time uses the service. This service model does have the largest part of the cloud computing industry and is expected to generate $117 billion in revenue by 2021, according research firm Gartner. It is now possible to utilize SaaS for a wide variety of purposes, including field service applications, system monitoring software, and scheduling tools.

Platform as a Service (PaaS):

Users are able to access a remote server using that allows them to build and share programs without the need for pricey IDE software to be installed on their local machines. Users may often tailor their subscription to include just the services they find most useful. According to Gartner's forecasts, by 2021, PaaS will have smallest market share of a three service categories, with revenues of about 27 billion USD. Providers of Platform as a Service (PaaS) including Microsoft Azure (also an IaaS), Google App Engine, and Apache Stratus now provide commercially available apps.

Infrastructure as a Service (IaaS)

When it comes to procuring IT resources on demand and through the internet, infrastructure as a service provides a standardized method. Data storage facilities, data networks, computers, as well as Virtual Private Servers (VPSs) are all types of resources. As the name implies, user will only pay for the resources they really use, such as the amount of storage space or computing power, and for the time period user actually utilize it. Under this service model, the provider takes care of maintaining the infrastructure and making sure it's available at all times, while the customer doesn't have to worry about a thing. According to Gartner, growth in this kind of service model will speed up to 35.9 percent next year. At now, only Amazon EC2 as well as Google Cloud Platform provides IaaS services.

1.4 Cloud security

Cloud security is a set of processes and technologies designed to handle external and internal enterprise security risks. As digital transformation plans move forward and cloud-based tools and services are incorporated into their infrastructure, enterprises need cloud-based security.One of the most important and quickly developing issues these days is cloud computing. It provides various types of benefits to different organizations such as computational and storage resources at affordable cost. As acceptance of cloud computing is increasing the security issues related to it are also increasing. Customers hesitate to move their business to the cloud due to security issues.

There are several risks associated with cloud computing such as loss control of data, multi-tenancy risk, security and privacy of data, and reliability issues. The rise of cloud computing services has led several organizations to take their large amount of information to the cloud. It brings out the requirement for the cloud's data to be secure and accurate. There are significant security problems posed by unauthorized individuals who access data.

Data that is saved in the cloud is no longer within the consumer's control because it is kept on the premises of the service provider. All the necessary controls are with the service provider such as identity management, security policies, and enforcement. Consumers rely on the provider to ensure data security and resource availability. It poses serious threats to privacy and security.

Multi-tenancy is a very useful feature of cloud computing where tenants share a pool of resources. There could be a malicious tenant who wants to exploit this system as he is on the same physical machine as others. There is a possibility that malicious users can steal others' confidential data if isolation is not done properly.

Data security is a critical aspect of cloud security, as data breaches have consistently remained a top threat in recent years. As the saying goes, “If the cloud is not secure, then the data stored within it is also at risk.” Data serves as the foundation and core of the cloud infrastructure, and breaches have been identified as the most serve threat by CSA (Cloud Security Alliance) since 2016 to date.

In cloud computing, the data has been very crucial and its security requires assurance. The data is placed at a distant location. It may be a different city, country, or continent. In an attempt to attain multi-tenancy, data leakage can occur. There are various stages of data where data is created, moved, utilized, shared, documented then finally deleted. The data requires being protected at all mentioned levels. Data level security has mainly two levels. The first level is when data is at moving and the final level is when data is at a steady position. The data at rest

position requires extra security precautions. The data movement is more secure as it is done by TLS. The data which lies idle tempts more attacks. Data at both levels have security challenges. The challenges require to be solved.

Various solutions can be used in securing data but most of them incurred extra costs in terms of storage, communication, and computational power. It is an issue when vulnerabilities are tackled and it raises the extra cost. There is a requirement for encryption techniques that are potent, adaptable, and safe with fine-grained access control. It will provide additional security with minimal extra cost.

1.4.1 Challenges of Cloud Security

This expanding cloud technology is encountering a great number of technical challenges in a variety of aspects of the data and information processing and storage processes. Few challenges are listed below:

Denial of Service (DoS)

Cloud providers are prime targets for malicious attacks as more organizations and businesses move their operations to the cloud. DDoS (Distributed Denial of Service) attacks have become more common than ever. According to VeriSign, the most targeted industries in the first quarter of 2015 were IT services, cloud platforms (PaaS) and SaaS. The purpose of a DDoS attack is to overload website servers so that they cannot properly process user requests. A DDoS assault may take down a website for hours or even days if it is successful. This may lead to a loss of sales, client confidence, and brand authority. Protecting a company against distributed denial of service attacks (DDoS) is no longer only a good idea; rather, it is a need. Websites and other web-based applications are essential for doing business in the 21st century and need the most advanced forms of cyber security (Kumari Poonam et al., 2021).

Data loss

When moving to the cloud, it’s wise to worry about the security of business-critical information. Loss of cloud data due to human error or inadvertent deletion, adversarial intervention such as malware installation (e.g. DDoS), or natural disaster that causes a cloud service provider to be offline can be catastrophic for an enterprise organization. DDoS attacks often serve simply as a distraction from more serious threats, such attempts to steal or erase data (Sharma Shubhanjali et al., 2014).

Insecure access control points

The ability to access the cloud from any location and on any device is one of its many advantages. However, if the user interface and especially the application programming interface (API) are not secure. Given enough time, hackers can find and access such vulnerabilities and use APIs for authentication. An HTTP request to a website is checked by a transactional web application's firewall to make sure it is genuine traffic. Web applications and APIs are protected by this always-on device against security lapses in cloud settings and off-site data centers.

Notifications and alerts

Network security, including cloud computing security, is based on security awareness and effective communication. A comprehensive data access control strategy should include notifying administrators of affected websites or applications of threats as soon as they are detected (Kumari Poonam et al., 2021).

1.4.2 Types of cloud security

There are two cloud security types as described below:

Centralized cloud Security

Environments for traditional on-premises business security are often decentralized. IT teams must manage and maintain security in decentralized settings for every site and application.

Unified Threat Management (UTM) describes a unified security system and appliance that performs many security tasks concurrently. However, utilizing cloud computing resources, enterprises may deploy a UTM system to oversee the security of both physical and virtual endpoints.

The whole company network is safeguarded by a single security strategy against external attacks. Spam filters, firewall configurations, spyware as well as virus protection, authentication, and virtual private network (VPN) setups are just some of the company-wide security measures that IT personnel may be responsible for monitoring the VPN. In addition to the time and money savings, centralizing security in the cloud also minimizes the requirement for on-premises hardware purchases as well as maintenance.

Centralized cloud security's aim is to instantly notify IT teams of a common threat. The threat is then removed with the use of a policy that is created from this notification. This procedure is

entirely automated; no humans are involved. Companies can be shielded by this proactive, automated method of protecting against both relatively harmless disturbances such Distributed Denial of Service (DDoS) assaults and much more dangerous threats like data breaches.

In general, a centralized security system consists of the following parts:

i. Firewall— remove any potentially harmful data from the network. Firewall centralization may be provided either on-premises or remotely via the cloud.

ii. VPN Networking— aids in hiding users online footprint by encrypting their communications. Virtual Private Networks (VPNs) are often used in centralized networking systems to encrypt data leaving the network.

iii. Load balancing— aid in peak traffic stabilization by directing data flows between the network's servers and database.

Limitations of a Centralized System

At a certain point, vertical scaling is not possible - Even if user upgrade the server node's hardware and software capabilities beyond a certain point, performance won't improve much, resulting in a cost-to-benefit ratio of less than one.

Due to the fact that server can only have so many listening ports, bottlenecks may form if a large number of client nodes attempt to connect to it at once. As a result, when the server is subjected to a large influx of visitors (like during a sale), it may suffer a DoS or DoS assault.

Distributed Cloud Security

The goal is to have the blockchain handle all aspects of cloud storage, from transferring data to processing and storing it (L. Jiang et al., 2022). Everyone with access to a blockchain may verify what happens to the information at a later date. By providing complete audit ability and visibility into cloud operations, this solution is ideal.

Using Distributed Cloud Architecture, users may store data in a safe, decentralized way (E. N. Witanto et al., 2021). This is accomplished through the use of blockchain technologies such as ledgers and public/private key encryption. These features return control to the user over their data and gadgets. Because it is distributed, no one server is at risk.

In order to create a high-performance cloud-based architecture that can handle future demands, it is important to keep the following in mind:

i. Resilience: Computation continues on some other nodes even if some nodes fail.

ii. Efficiency: Users benefit from top-notch speed even while working with nodes that have varying degrees of homogeneity.

iii. Ease of deployment: Each node may be placed independently of the others during deployment.

iv. Adaptability: To keep up with the ever-increasing demands of the client base, the network's design must be flexible enough to adapt to new conditions and new applications.

v. Performance: In a decentralized system, linear performance is essential.

vi. Security: Information privacy, secrecy, and security are all crucial and must be properly handled.

Limitations of Distributed Systems

Designing and debugging algorithms for the system is challenging. Because there is no common clock, it is difficult to utilize these algorithms because there can be no chronological ordering of commands or logs. When developing such algorithms, nodes may have varying latencies, which must be taken into consideration. As the number of nodes rises, so does the complexity. For further details, click this site. The chronological arrangement of events and transactions is complicated by the absence of a common clock. It's hard for a single node to know everything about the system and, as a result, to make decisions depending on the states of other nodes.

2. LITERATURE REVIEW

S. Jegadeeswari et al. (2019) suggested cloud data storage using a dynamic bloom filter (DBFH-CDS). The DBFH-CDS Method was developed with the intention of bolstering the privacy and safety of cloud-based data storage. The proposed method makes use of a Bloom filter and a data fragmentation model. The DBFH-CDS Method utilizes a data fragmentation model to break up large cloud datasets. The DBFH-CDS Method then employs the Bloom Filter to safely store the data fragments containing the sensitive information. The DBFH-CDS Method, which makes use of the Bloom Filter, provides excellent protection and privacy for cloud data storage. The efficiency and speed with which data is retrieved are two measures used to evaluate the proposed DBFH-CDS Technique. The results of the evaluations show promise that DBFH-CDS Technique may improve cloud digital storage security without increasing storage requirements when compared to prior art methods.

J. Jeong et al. (2019) study provides cloud-based data security for the Internet of Things that uses Bloom filters and thus is founded on a verified model of data ownership. The results of the experiments show that the proposed approach is efficient and produces similar verification rates to the present techniques, even when the Bloom filter generates false positives. As a result, the suggested service can analyze a huge volume of data created in an IoT context efficiently.

Ming Zeng et al. (2019) have explained "Public Key Encryption with Keyword Search (PKSE)". When a client generates the search token for the first time while requesting the data, the cloud service provider uses a discovery token before requesting the encrypted data followed by the data files. However, a significant attack occurs when searching in the PKSE cloud. The cloud server can retrieve the information about the add new notification files, keywords too in addition to the search code already found, and also search for privacy information. To solve this problem, the authors use straightforward secure encryption. To address this problem, the authors propose a direct secure encryption scheme with the public key and discovery, and also a framework for generating direct secure encryption schemes with the public key and feature-based discoverable encryption.

Y. Changsong et al. (2020) develop a novel counting Bloom filter-based strategy for safely transferring information from cloud storage to another and then erasing it forever from the source cloud. The suggested approach not only allows for safe data transit but also permanent data erasure. Furthermore, the suggested system may fulfill public verifiability without the need for a

trusted third party. After laying out the idea, the author develops a virtual implementation to demonstrate its viability and effectiveness.

Yingying Li et al. (2020) have explained Content Based Image Extraction (CBIR). This feature attracted a lot of attenqtion in many fields. On the other hand, existing CBIR privacy protection programs provide image privacy that is guaranteed with photo backup, acquisition, although these plans still have shortcomings. To address these problems, the authors propose parallelism research for an encrypted image in secure cloud computing. Authors explain convolution neural network, encrypted sequential code tree using K-mean clustering based on contact-diffusion clustering and explain k- nearest neighbor (kNN).

S. Tanwar et al. (2020) suggested User Access Policies Algorithm enhances healthcare provider data access and simulates settings to develop a Continuous and constant electronic healthcare record that uses chain code. For better results, blockchain networks have enhanced latency, throughput, & RTT. Blockchain outperforms client-server EHR alternatives in efficiency and security.

O. I. Khalaf et al. (2021) uses verified data ownership to substitute actual electronic currency for mining then store fresh data sets to compare to the research model, significantly decreasing computer capacity. ODSD protects dynamic data storage for real-time applications.

D. Samanta et al. (2021) created a computationally safe operating system to encrypt data. In the first phase, an SVM-based encryption service model with improved key generation is created. In descendant two approaches application model that is computationally more secure for Cloud environment, optimization techniques are used for key generation. The results showed that the suggested application model can survive Selected Cipher Attack, Plain Text Attack, and other file assaults. Whereas visuals withstand statistical and differential assaults. Comparative Analysis reveals the pioneering application model's efficiency and strength compared to current services.

G. N. Nguyen et al. (2021) discussed how intruders are detected using sensor data collected by deep belief network models. The approach generates several picture shares using an include how creation methodology, ensuring privacy and security. In order to identify illness, a residue network-based classification algorithm is performed in the cloud, where it is protected by blockchain technology. Users put the model through its paces on the NSL-KDD 2015, CIDDS-001, as well as ISIC datasets.

R. Kumar et al. (2021) provided the copyright violations which were underlined to protect copyright holders. Photographers, producers, & graphic artists transmit millions of photos and films every day. Grayscale conversion, cutting, rotating, frame compression, & clip speed modify multimedia. Upload corrupt files. Share photographs & media on IPFS. Perceptual hash identifies multimedia copyright infringement of pHash. IPFS multimedia utilizes blockchain hashes. Blockchain skips middlemen utilizing pHash-like media.

W. Li et al. (2021) investigated blockchain-based cloud computing trust techniques. It highlights outstanding difficulties and suggests further study using a novel cloud transaction architecture based on a double-blockchain structure and cloud edge trust management.

A. Lakhan et al. (2021) advised securely offloading all duties with Linear search-based task scheduling (LSBTS) maps all tasks to suitable computational nodes to provide application Quality of Service (QoS). The experimental findings demonstrated devise strategies surpass all other approaches to the issue.

Summary of literature review is shown in Table 1.

Table 1 Summary of literature review

Title of Paper	**Year/ Journal**	**Methodology**	**Research Gap**	**Outcomes**
"Efficient Dynamic Bloom Filter Hashing Fragmentation for Cloud Data Storage"	Cybernetics and Information Technologies, 2019	The Java language and the bank marketing dataset from the UCI machine learning repository form the basis of the (DBFH-CDS) method.	Lack of exploration regarding how the DBFH-CDS method's security is impacted when fragments undergo encryption using different cryptographic techniques. Despite its enhanced security claims, there's a need to empirically evaluate and compare the effectiveness of the DBFH-CDS	Compared to existing research, it is clear that cloud data storage capabilities produce more accurate results.

			method against existing approaches in cloud data storage accuracy.	
"Secure Cloud Storage Service Using Bloom Filters for the Internet of Things"	IEEE Access 2019 (Open Access)	Cloud-based data security for the Internet of Things based on a PDP method using a Bloom filter	The methodology focuses on security and efficiency, practical validation of its effectiveness in real IoT data scenarios remains unexplored	The suggested service can analyze a huge volume of data created in an IoT context efficiently.
"Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage"	IEEE transactions on cloud computing, 2019	Cryptographic Approach	There is a need for a detailed assessment and evaluation of the efficacy and security implications of public key-recognizable encryption.	Using direct secure encryption scheme to secure data through tokens
"Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing"	Chinese Journal of Electronics, 2020	A safe method of transmitting information using CBF,	There is lack of exploration into securely transferring information from a source cloud to multiple destination clouds using Counting Bloom Filters (CBF).	Accomplish safe data sharing and be able to delete information for good.
"Similarity Search for Encrypted Images in secure Cloud Computing"	IEEE Transactions on Cloud Computing, 2020	Content-Based Image Retrieval	There is a requirement for addressing privacy protection issues in Content-Based Image Retrieval (CBIR) and K-cluster methodologies when applied to encrypted images in secure cloud computing.	Parallelism research for an encrypted image in secure cloud computing.

"Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions"	Journal of Cloud Computing, 2021	A comprehensive review of blockchain based trust approaches in cloud computing systems.	The gap identified is the significant disparity between legal theory and its practical implementation in blockchain-based trust management within cloud computing systems.	Review the application block for credibility.
"Mobility Aware Blockchain Enabled Offloading and Scheduling in Vehicular Fog Cloud Computing"	IEEE Transactions on Intelligent Transportation Systems, 2021	The new vehicular fog cloud network (VFCN) consists of various components and heterogeneous computing nodes.	There is insufficient exploration of budgeting and fault tolerance aspects specifically related to IoT applications within the Vehicular Fog Cloud Network (VFCN).	The proposed scheme is better in terms of cost, safety and time as compared to the existing state-of-the-art systems

2.1 Research Gaps

- Integration of blockchain with the Interplanetary File System (IPFS) is essential for robust file encryption in cloud-based data security. Existing research falls short in addressing the challenges and opportunities of this combination, limiting a thorough exploration of its potential for enhanced data protection.
- Current studies lack emphasis on user-centric security measures and fail to elucidate how unique user addresses contribute to individualized control, leaving a gap in understanding their impact on overall data security.
- Optimization of the Cloud Record Manager is necessary for streamlined record management on decentralized cloud storage, aiming to enhance both performance and security of this critical component.
- Challenges arise in the exploration of consensus algorithms and data storage technologies to expedite transaction processing and improve the efficiency of data queries.
- There is a requirement for a comprehensive evaluation of security enhancements utilizing blockchain technology in distributed processing systems.

- Difficulties persist in assessing the potential of blockchain technology to establish a secure and reliable framework for data sharing in distributed processing systems.
- There is a deficiency in addressing scalability challenges in practical scenarios, encompassing factors such as transaction volume, network size, and resource constraints.

3. CLOUD SECURITY USING BLOCKCHAIN

A blockchain is "an encrypted, decentralized, and ever-growing collection of records, called blocks," which are linked together (K. Fanning et al., 2016). Each block contains information about a transaction, a timestamp, and even the cryptographic digest of a prior block. Transactions are recorded in a distributed public blockchain called a blockchain that is shared across many computers in a manner that prevents any one node from modifying the ledger without updating all subsequent nodes, which would then invalidate the network consensus (A. Lakhan et al., 2021). Benefits of the blockchain are as follows:

i. Full decentralization and real redundancy: Using blockchain, a decentralized system for cloud storage in data which is stored on a network comprising thousands of computers at key locations throughout the globe can be designed.

ii. Transparency: All parties can see and modify information on blockchains. As a result, fraud and risk are reduced, and confidence is boosted.

ii. Security: Because of its decentralized nature, blockchains very difficult to compromise.

iv. Fewer Intermediaries: Because blockchain is decentralized and depends on trust between users, it lowers dependency on third-party intermediaries such as banks, brokers, gateways, and so on.

v. Automation: Because blockchain is programmable, In the case that certain conditions are met, it may initiate a predetermined course of action.

vi. Faster Processes: Because of blockchain's ability to speed up process execution within multi-party scenarios, transactions are no longer limited to business hours.

Establishing and deploying a private blockchain on a trustworthy and secure platform is of utmost importance, as poorly matched underlying technology for business needs and processes can expose data security vulnerabilities.It is crucial not to overlook the risks associated with sound corporate governance and running a corporation, including threats to the company's financial stability, reputation, and legal compliance. Due to the decentralized nature of blockchain systems, they are susceptible to governance challenges, necessitating strict regulation of decision-making processes, guiding principles, identity management, and access permissions.

The security of a blockchain network relies on the timely detection and mitigation of potential threats, guided by a comprehensive blockchain security concept. Developing a blockchain security model ensures the adequate protection of user blockchain solutions.

To implement a secure blockchain system, administrators must first formulate a risk model capable of addressing issues across the business, governance, technology, and process domains. Subsequently, a threat model should be created to assess the risks associated with employing the blockchain solution. Finally, administrators must establish security measures that mitigate risks and threats, categorized under one of the three main categories:

i. Enforce blockchain-specific security measures.
ii. Implement customary security measures.
iii. Enforce business controls for blockchain.

3.1 Blockchain network types

Consortium blockchains: In a consortium blockchain, a predetermined body, such as a collection of businesses, oversees the consensus process. The public or just those who are members of the network may access the blockchain and add new transactions to it. A consortium blockchain, sometimes known as a "permissioned blockchain," is a blockchain that may only be accessed by an author's organization (O. Dib et al., 2018).

Semi-private blockchains: If user's match the requirements they may join a semi-private blockchain that is maintained by a single company. In spite of its lack of decentralization, this permission blockchain presents an attractive option for use in public sector contexts (I. Radanović et al., 2018).

Private Blockchains: In private blockchains, a central authority decides who may see the ledger and take part in the network's consensus. They are only suitable for usage as sandboxes and not in production because of their centralization (T. Tuan et al., 2020).

Public Blockchains: A public blockchain allows anybody with internet access to observe the ledger and take part in reaching a consensus. They are considered to have "less authorization." Users may remain anonymous while their transactions are publicly viewable. Well-known examples of public blockchains are Bitcoin and Ethereum (D. Guegan, 2017).

A blockchain is, as the name indicates, a network of digital blocks which records financial transactions. A particular block is connected to all the blocks that come before and after it. Since of this, it's hard to change just one record without being caught since hackers would have to change the block containing the record as well as the blocks related to it. This may not seem to be much of a barrier, but blockchain has other inherent traits that provide additional safety features.

The data on a blockchain is encrypted for safety. Each user in the network has their own private key, which serves as a digital signature for their transactions. A peer network will be alerted promptly if a record is modified and its signature is no longer valid. The key to preventing more damage is early notice.

Unfortunately for the enthusiastic hackers, blockchain are scattered across peer-to-peer networks which are constantly updated and maintained in sync. Since blockchain aren't stored in a central place, there is no single point of failure, and no one system can make changes to the ledger. Huge amounts of computing power would be required to get access to all instances of a given blockchain and make simultaneous changes to them all. Although the possible attack ability of smaller blockchain networks has been addressed, no firm conclusion has been made as of yet.

3.2 Problem statement

This research endeavors to tackle the mounting challenges in cloud-based data security through the design and implementation of a sophisticated system utilizing distributed blockchain technology. Therefore problem statement is defined as:

Design a novel algorithm for a secure and reliable blockchain-based distributed data security system for cloud computing to enhance the efficiency and performance of the system by leveraging distributed processing.

4. RESEARCH OBJECTIVES

Research objectives play a pivotal role in any research study as they define its purpose and scope. They offer a clear understanding of the researcher's intentions and what they aim to accomplish through the study. Presented below are the research objectives:

1. To study and understand the existing blockchain-based distributed data security system for cloud computing.

2. To propose a novel blockchain-based distributed data security algorithm to enhance the security in cloud based system.

3. To implement the proposed algorithm in terms of its accuracy, scalability, and performance.

4. To evaluate the effectiveness of the proposed algorithm in terms of efficiency and performance.

5. RESEARCH METHODOLOGY

The research methodology encompasses the comprehensive process of strategizing, designing, executing, analyzing, and interpreting research studies. It entails the thoughtful selection of suitable research methods, tools, and techniques that align with the research objectives. Presented below is the research methodology:

1. Study of literature review on cloud computing security.

2. Study of available tools, mechanisms, challenges and categorizing the issues of cloud security. An analysis and comparison of existing techniques based on advantage and disadvantage of cloud computing security. Identify area of improvisation to make cloud security is more usable for the users.

3. Implementation of a distributed blockchain technology will be proposed for optimizing the existing techniques and implemented in Python which will be used to encrypt the data for unauthorized access. In the proposed technique data object will be protected with hash algorithm using data encryption standard.

4. Comparative performance analysis of the proposed algorithm with the existing algorithms will be done.

The proposed methodology is based on the following approach and Fig. 1 depicts the design of the proposed system:

Step 1: Initialize the system and establish a blockchain network. Encrypt the user's file using the Interplanetary File System protocol (IPFS).

Step 2: Generate and assign a unique address to the local user on the blockchain network and ensure that the network is private and controlled by a single local user.

Step 3: Store the user's address on the blockchain to maintain privacy and security and transmit the encrypted user's file to other peers in the blockchain network.

Step 4: Each machine in the blockchain network holds a copy of the distributed ledger, ensuring the original state of the blockchain is secure from tampering.

Step 5: Set up a Cloud Record Manager for efficient record management.

Step 6: Store extensive information on the decentralized cloud storage, ensuring data privacy and security. When a participating organization needs to retrieve a specific record; they must have the public address of the user on the blockchain network.

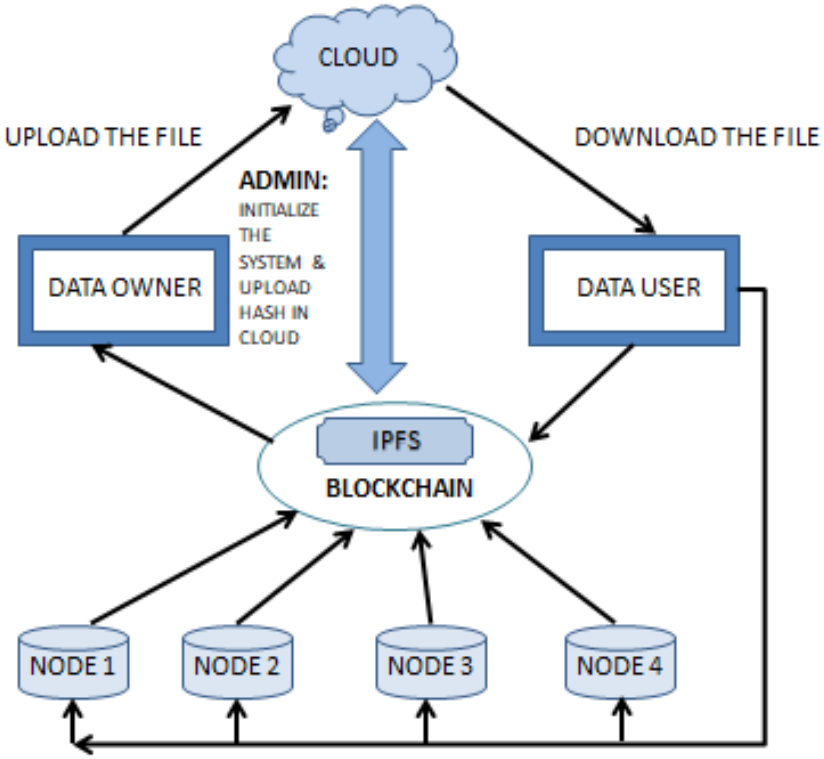

Fig. 1 System Design for Decentralized Cloud Storage (M. Naz et al., 2019)

6. EXPECTED OUTCOME OF THE RESEARCH

The suggested method will link a user's wallet address to a file such that only the owner has access to it. Ethereum's blockchain is where user information is stored. Smart contracts can be used on the Ethereum blockchain network to record details about user-uploaded files. The proposed system may encrypt and decode data at every data transfer. The IPFS Protocol is used to facilitate the system's efficient file sharing across its many network partners.

REFERENCES

[1] A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood (2021), 'Mobility Aware Blockchain Enabled Offloading and Scheduling in Vehicular Fog Cloud Computing', *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4212–4223, doi: 10.1109/TITS.2021.3056461.

[2] B. K. Mohanta, U. Satapathy, S. S. Panda, and D. Jena (2020), 'A Novel Approach to Solve Security and Privacy Issues for IoT Applications using Blockchain', pp. 394- 399, no. June 2020, doi: 10.1109/ICIT48102.2019.00076.

[3] D. C. Wyld and Robert Maurin (2009), 'Moving to the Cloud : An Introduction to Cloud Computing in Government E-Government Series Moving to the Cloud : An Introduction to Cloud Computing in Government', *IBM Cent. Bus. Gov.*, no. February, pp. 82.

[4] D. Grzonka, J. Kołodziej, J. Tao, and S. U. Khan (2015), 'Artificial Neural Network support to monitoring of the evolutionary driven security aware scheduling in computational distributed environments', *Futur. Gener. Comput. Syst.*, vol. 51, pp. 72–86, doi: 10.1016/j.future.2014.10.031.

[5] D. Guegan (2017), 'Public Blockchain versus Private blockhain', *To cite this version : Centre d Economie de la Sorbonne Documents de Travail du Public Blockchain versus Private blockhain*, pp. 1-6.

[6] D. Samanta et al.(2021), 'Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture', *IEEE Access*, vol. 9, pp. 98013–98025, doi: 10.1109/ACCESS.2021.3095297.

[7] E. N. Witanto and S. Lee (2021), 'IoT A Conceptual Architecture in Decentralizing Computing , Storage , and Networking Aspect of IoT Infrastructure', pp. 205–221.

[8] Ghania AI Sadi (2015), 'Cloud Computing Architecture and Forensic Investigation Challenges' *International Journal of Computer Applications* (0975 –8887), vol. 124, no.7, pp. 20-25.

[9] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. Gupta, and A. El-Latif (2021), 'Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model', *J. Parallel Distrib. Comput.*, vol. 153, pp. 150–160, doi: 10.1016/j.jpdc.2021.03.011.

[10] G. Rathee, C. A. Kerrache, and M. A. Ferrag (2022), 'A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems', *J. Sens. Actuator Networks*, vol. 11, no. 4, pp. 71, doi: 10.3390/jsan11040071.

[11] I. Radanović and R. Likić (2018), 'Opportunities for use of blockchain technology in medicine', vol. 16, pp. 583–590.

[12] J. Zhu, Z. Zhang, C. Zhao, and T. Wang (2018), 'An infrastructure framework for privacy protection of community medical internet of things', *World Wide Web*, pp. 33-57, doi: 10.1007/s11280-017-0455-z.

[13] J. Jeong, J. W. J. Joo, Y. Lee, and Y. Son (2019), 'Secure cloud storage service using bloom filters for the internet of things', *IEEE Access*, vol. 7, pp. 60897–60907, doi: 10.1109/ACCESS.2019.2915576.

[14] K. Fanning and D. P. Centers (2016), "Blockchain and Its Coming," pp. 53–57, doi: 10.1002/jcaf.

[15] Kumar Kanishk (2018), 'Distributed cloud storage with blockchain technology', *Dell EMC Proven Professinal Knowledge Sharing*, pp. 1-11.

[16] Kumari Poonam, Singh Meeta (2021), 'A Review: Different Challenges in Energy – Efficient Cloud Security', *IOP Conf. Series: Earth and Environmental Science* **785,** pp. 1-10, 012002, IOP Publishing doi:10.1088/1755-1315/785/1/012002.

[17] Kumari Poonam, Singh Meeta (2021), 'Cloud Security and Challenges', *Review Of International Geographical Education* (RIGEO), 11(8), pp- 1866-1874, doi: 10.48047/rigeo.11.08.162.

[18] L. Jiang and Z. Qin (2022), 'Privacy-Preserving Task Distribution Mechanism with Cloud-Edge IoT for the Mobile Crowdsensing', *Secur. Commun. Networks*, vol. 2022, pp. 1-13, Article ID 6754744, doi: 10.1155/2022/6754744.

[19] M. A. Vouk (2008), 'Cloud Computing – Issues , Research and Implementations', *Journal of Computing and Information Technology - CIT*, vol. 16, no. 4, pp. 235–246.

[20] M. Niranjanamurthy, B. N. Nithya, S. Jagannatha (2019), 'Analysis of Blockchain technology pros , cons and SWOT _ new document', *Cluster Computing*, vol. 22, no. 6, pp. 14743-14757, https://doi.org/10.1007/s10586-018-2387-5.

[21] Ming Zeng, Haifeng Qian, Jie Chen, and Kai Zhang (2019), 'Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage', *IEEE*, pp. 436- 438, 2019.

[22] Naz, M., Al-zahrani, F.A., Khalid, R., Javaid, N., Qamar, A.M., Afzal, M.K. and Shafiq, M., 2019. A secure data sharing platform using blockchain and interplanetary file system. *Sustainability*, *11*(24), p.7054.

[23] O. Dib, K. Brousmiche, A. Durand, E. Thea, and E. Ben Hamida (2018), 'Consortium Blockchains : Overview , Applications and Challenges', International Journal on Advance Telecommunication, vol. 11, no. 1, pp. 51- 64, 2018.

[24] O. I. Khalaf and G. M. Abdulsahib(2021), 'Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks', *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2858–2873, doi: 10.1007/s12083-021-01115-4.

[25] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong (2021), 'A secured distributed detection system based on IPFS and blockchain for industrial image and video data security', *J. Parallel Distrib. Comput.*, vol. 152, pp. 128–143, doi: 10.1016/j.jpdc.2021.02.022.

[26] Sharma Shubhanjali, Gupta Garima and P.R. Laxmi (2014), 'A survey on cloud security issues and techniques', *International Journal on Computational Science and Application* vol. 4, no. 1, pp. 1 - 8.

[27] S. Jegadeeswari, P. Dinadayalan, and D. Gnanambigai (2019), 'Efficient dynamic bloom filter hashing fragmentation for cloud data storage', *Cybern. Inf. Technol.*, vol. 19, no. 1, pp. 53–72, doi: 10.2478/CAIT-2019-0003.

[28] S. Tanwar, K. Parekh, and R. Evans (2020), 'Blockchain-based electronic healthcare record system for healthcare 4.0 applications', *J. Inf. Secur. Appl.*, vol. 50, pp. 102407, doi: 10.1016/j.jisa.2019.102407.

[29] T. Tuan, A. Dinh, J. Wang, G. Chen, R. Liu, and C. Ooi (2020, 'BLOCKBENCH : A Framework for Analyzing Private Blockchains', pp. 1085–1100.

[30] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya (2021), 'Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions', *Journal of Cloud Computing*, vol. 10, no. 1, pp. 1- 35, doi: 10.1186/s13677-021-00247-5.

[31] Yingying Li, Jianfeng Ma, Yinbin Miao, Yue Wang, Ximeng Liu, and Kim-Kwang Raymond Choo (2020), 'Similarity Search for Encrypted Images in Secure Cloud Computing', *IEEE*, vol. 10, no. 2, pp. 1142- 1155, 2020.

[32] Y. Changsong, Y. Changsong, T. Xiaoling, Z. Feng, and W. Yong (2020), 'Secure data transfer and deletion from counting bloom filter in cloud computing', *Chinese J. Electron.*, vol. 29, no. 2, pp. 273–280, doi: 10.1049/cje.2020.02.015.

[33] Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen (2018), 'DivORAM: Towards a practical oblivious RAM with variable block size', *Inf. Sci. (Ny).*, vol. 447, pp. 1–11, doi: 10.1016/j.ins.2018.02.071.

MANAV RACHNA
Vidyavanodaribhavah

Dr. O.P. Bhalla Central Library
Manav Rachna International Institute of Research and Studies
(A deemed-to-be-university under section 3 of UGC Act 1956)

SIMILARITY VERIFICATION CERTIFICATE

Title: Design of Blockchain - Based Algorithm for Cloud Data Security

Researcher: Poonam Kumari Registration Number: 19/Ph.D/106

Supervisor: Dr. Mecta Singh Department: Computer Science & Engineering

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through Turnitin Software on 5/03/2026 with submission ID no. id: 3498361819 and the similarity index was found to be 5 %. The complete report running into 28 Pages, 7,7412 Word count with File Size 160.5 KB/MB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date:

Dr. Rajesh Kumar
University Librarian
Dr. O.P. Bhalla Central Library
Manav Rachna International
Institute of Research & Studies
Faridabad

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

Research Scholar
Poonam Kumari

Research Supervisor

turnitin Page 5 of 32 - Integrity Submission Submission ID trn:oid:::1:3498361959

Design of Blockchain - Based Algorithm for Cloud Data Security

SHORT SYNOPSIS

by

POONAM KUMARI

(19/Ph.D/106)

Under the supervision of

Dr. Meeta Singh

Professor, Computer Science & Engineering

SCHOOL OF ENGINEERING & TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD

ABSTRACT

Nowadays, Cloud Computing is the fastest-growing IT technology which is rising day by day because of its flexibility & easy to use features. Cloud Computing provides the ability to reduce the cost of pay-per-use and increases scalability. When a user demands any resource or service like software, hardware, or infrastructure in cloud computing then that will be provided as per the request. The major concern is the data security in cloud computing, as the data will be stored by a third party & easily accessible through the internet. Many security issues can arise due to the invisibility of data as there is no full control over data by the customer. Therefore, there is a need for cloud security which must ensure the protection of the user data on the cloud.

turnitin Page 5 of 32 - Integrity Submission Submission ID trn:oid:::1:3498361959

Submission ID trn:oid:::1:3498361959

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Small Matches (less than 12 words)

Exclusions

- 1 Excluded Source

Excluding matches less than 14 words

Dr. Rajesh Kumar
University Librarian
Dr. O.P. Bhalla Central Library

Match Groups

- 11 Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- 1 Missing Quotations 0%
  Matches that are still very similar to source material
- 6 Missing Citation 1%
  Matches that have quotation marks, but no in-text citation
- 1 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
3% Publications
4% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

9/03/2026

Submission ID trn:oid:::1:3498361959

atch Groups

- 11 Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- 1 Missing Quotations 0%
  Matches that are still very similar to source material
- 6 Missing Citation 1%
  Matches that have quotation marks, but no in-text citation
- 1 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
3% Publications
4% Submitted works (Student Papers)

Excluding matches less than 14 words

Dr. Rajesh Kumar
University Librarian
Dr. O.P. Bhalla Central Library
Manav Rachna International Institute of Research & Studies
Faridabad

op Sources

he sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Publication	
Deepak Kumar Acharya, Manish Shrivastava, Payodhar Padhi. "A Decentralized Bl...		<1%
2	Student papers	
University of Wales Institute, Cardiff		<1%
3	Student papers	
Kaplan International Colleges		<1%
4	Internet	
www.research.lancs.ac.uk		<1%
5	Internet	
shodh.inflibnet.ac.in:8080		<1%
6	Student papers	
University of East London		<1%
7	Internet	
www.hindawi.com		<1%
8	Internet	
lorojournals.com		<1%
9	Internet	
www.jatit.org		<1%
10	Internet	
onlinelibrary.wiley.com		<1%

11	Internet kiv.org	<1%
12	Student papers obal University	<1%
13	Internet eo.org	<1%
14	Internet ww.mdpi.com	<1%
15	Internet positorio.ucv.edu.pe	<1%
16	Internet ww.paspk.org	<1%
17	Internet rary.ndsu.edu	<1%